BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-261483
(43)Date of publication of application : 22.09.2000

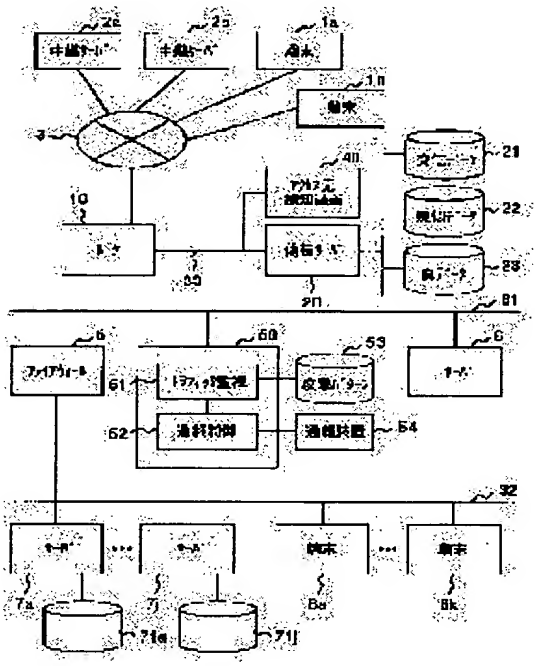
(51)Int.Cl. H04L 12/46
H04L 12/28
G06F 13/00
H04L 12/24
H04L 12/26
H04L 12/56

(21)Application number : 11-061185
(22)Date of filing : 09.03.1999

(71)Applicant : HITACHI LTD
(72)Inventor : IDEMOTO MANABU

(54) NETWORK MONITORING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a network monitoring system where an illegal access from an external network to an in-enterprise information network can be detected and a transmission source of an illegal packet can be retrieved.
SOLUTION: The network monitoring system is provided with a traffic monitoring device 50 that monitors traffic of a packet passing through a router 10 and received from an external network 3 and informs the router about identification information of an illegal packet at the time of detecting the illegal packet and with a disguised server 20 that gives a false reply to a sender of the illegal packet. The router 10 identifies the illegal packet coming from the external network and transfers the illegal packet to the disguised server based on the identification information of the illegal packet informed from the monitoring device.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

JP 2000 - 261483 Network Monitoring System

【Claim 1】 A network surveillance system for watching for illegal access from an outside network to an internal information network which is connected to the outside network by way of a router, the network surveillance system comprising:

a traffic surveillance apparatus, which watches an inflow traffic of packets from the outside network by way of the router, and upon detection of a packet illegally accessing the internal information network, transmits a control packet indicating an identification information of the illegal packet to the router device; and

a false server, which responds to a packet received, and transmits a response packet including intentional information to a transmitting source of the packet received ,

wherein the router is provided with means for responding to the control packet received from the surveillance apparatus and storing the identification information of the illegal packet, and wherein the router identifies the illegal packet based on the identification information from among packets received from the outside network, and transfers it to the false server.

Nikkei Communications 9/20, 1999,
Feature 94, "Security Measures Handled by Specialists"

①FIG. 1-3 THERE ARE THREE TYPES OF FIREWALL MANAGEMENT REPRESENTATIVE SERVICES: "HOSTING TYPE" IN WHICH FIREWALL IS INSTALLED IN A PROVIDER'S FACILITY AND AN OPERATOR CONTROLS IT FOR MANAGEMENT AND SURVEILLANCE, "REMOTE CONTROL MANAGEMENT TYPE" WHICH IS A VARIATION OF THE "HOSTING TYPE" AND IN WHICH AN OPERATOR CONTROLS IT FROM A DISTANCE FOR MANAGEMENT AND SURVEILLANCE, AND "ECONOMY TYPE" IN WHICH A LOW COST MACHINE DESIGNED FOR FIREWALL IS CONTROLLED FROM A DISTANCE FOR MANAGEMENT AND SURVEILLANCE.

②FIREWALL DESIGNED FOR USER IS INSTALLED IN THE NOC OR MANAGEMENT CENTER OF A PROVIDER, AND CONTROLLED BY AN OPERATOR FOR MANAGEMENT AND SURVEILLANCE.
●SERVICE CHARGES BECOME HIGHER WITH INDIVIDUAL USER-ORIENTED SERVICES
●CUSTOMIZATION BECOMES HIGH ACCORDINGLY. USED IN MANY CASES WITH THE HOSTING OF A WWW SERVER MAIL SERVER.

③AN OPERATOR CONTROLS FIREWALL INSTALLED ON THE USER SIDE FROM A DISTANCE FOR MANAGEMENT AND SURVEILLANCE.
●A VARIATION OF THE HOSTING TYPE, AND USED IN THE CASE OF NO FIREWALL INSTALLABLE ON THE PROVIDER SIDE.
●BECAUSE OF REMOTE CONTROLLED MANAGEMENT FAULT HANDLING IS DONE LATER THAN THAT OF THE HOSTING TYPE

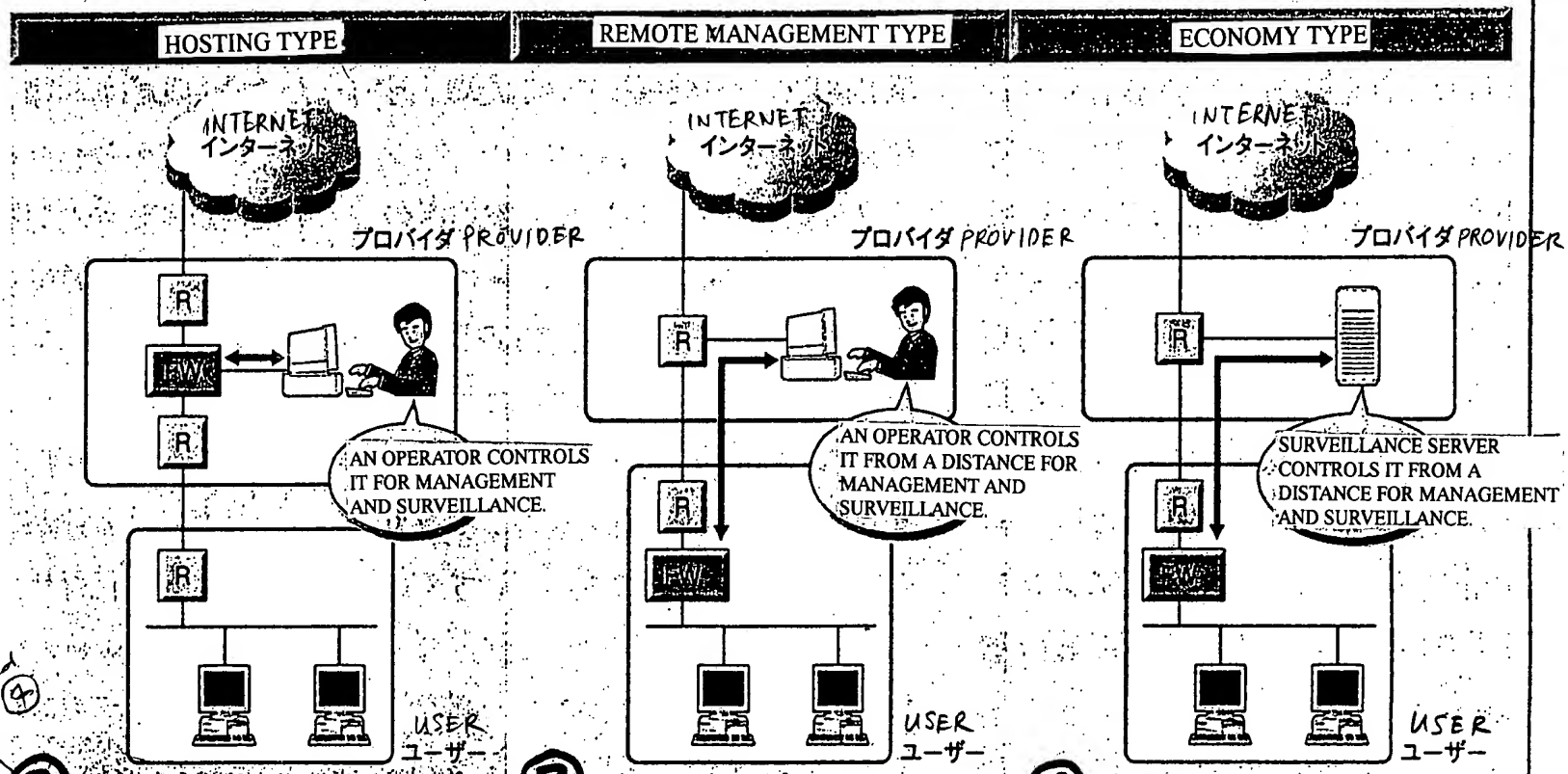
④A SURVEILLANCE SERVER CONTROLS FIREWALL INSTALLED ON THE USER SIDE FROM A DISTANCE FOR MANAGEMENT AND SURVEILLANCE
●PRICE IS LOWERED WITH STYLIZED MANAGEMENT AND STAFFS SLASHED.
●USE LOW-COST MACHINE DESIGNED FOR FIREWALL.
●CUSTOMIZATION BECOMES LOW.

Feature 94, "Security Measures Handled by Specialists"
- Exploration of Practicability of Outsourcing -
Internet Firewall Security Checkup
(*Nikkei Communications* 9/20, 1999)

In an economy-type management representative service, instead of a man checking but a surveillance server checks out such as illegal access automatically. The mechanism is that based on alert information received from a firewall, the surveillance server analyses a log and notifies the user of it.

① See attached ①

図1-3　ファイアウォール運用代行サービスは3タイプある　ファイアウォールをプロバイダの設備に収容してオペレータが運用・監視する「ホスティング型」，その変形版で遠隔地からオペレータが運用・監視する「リモート運用型」，および安価なファイアウォール専用機を監視サーバーで遠隔地から運用・監視する「エコノミー型」がある。



See attached ③-④

OUTLINE 概要	② ユーザー専用のファイアウォールをプロバイダのNOCや運用管理センター内に設置し，オペレータが運用・監視する	③ ユーザー側に設置したファイアウォールを，オペレータが遠隔地から運用・監視する	④ ユーザー側に設置したファイアウォールを，監視サーバーが遠隔地から運用・監視する
FEATURES 特徴	●ユーザーごとの個別対応的な要素が強く，利用料金は高めになる ●その分カスタマイズ性は高い。WWWサーバーやメール・サーバーのホスティングと併用するケースも多い	●ホスティング型の変形版で，プロバイダ側にファイアウォールを置けない場合に利用する ●遠隔地からの運用になるため，障害発生時の対応はホスティング型よりも遅くなる	●運用を定型化し，人手を減らして低価格化 ●安価なファイアウォール専用機を利用する ●カスタマイズ性は低い
SERVICE CHARGE PER MONTH 月額利用料金	300,000-1,000,000 OR MORE	150,000-1,000,000 OR MORE	AROUND 50,000-60,000
SIZE OF THE USER ユーザーの規模	MEDIUM-LARGE (MAINLY 500-1000)	MEDIUM-LARGE (MAINLY 500-1000)	SMALL-MEDIUM (ABOUT UP TO 500)

NOC:ネットワーク・オペレーション・センター NETWORK OPERATION CENTER　FW:ファイアウォール FIREWALL　R:ルーター ROUTER